JP2002259344 A

ONE-TIME PASSWORD AUTHENTICATION SYSTEM, PORTABLE TELEPHONE AND USER IDENTIFICATION SERVER

MITSUBISHI ELECTRIC CORP

Inventor(s):YONEDA TAKESHI

Application No. 2001053911 JP2001053911 JP, Filed 20010228,A1 Published 20020913Published 20020913

Abstract: PROBLEM TO BE SOLVED: To easily manage secret information while securing the safety of a one-time password concerning user authentication using the one-time password in an information communication network system.

SOLUTION: A hush generation part 113 in a portable telephone set 101 obtains a hush value by using a user ID, present time information and common secret information and generates the one-time password. In a user authentication server 103 receiving the user ID and the one-time password from a user PC 102, a hush generation part 124 generates the one-time password similarly by using the received user ID, the present time information and the common secret information to use it for verification by a one-time password verification part.

Int'l Class: G06F01500; H04B00726 H04Q00738 H04L00932 H04Q00734

Patents Citing this One: No US, EP, or WO patents/search reports have cited this patent. MicroPatent Reference Number: 000618317

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－259344
（P2002－259344A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｂ　7/26		Ｈ０４Ｂ　7/26	Ｍ	５Ｊ１０４
Ｈ０４Ｑ　7/38			１０９Ｓ	５Ｋ０６７
Ｈ０４Ｌ　9/32			１０９Ｍ	
Ｈ０４Ｑ　7/34		Ｈ０４Ｌ　9/00	６７３Ｃ	

審査請求　未請求　請求項の数８　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2001－53911(P2001－53911)

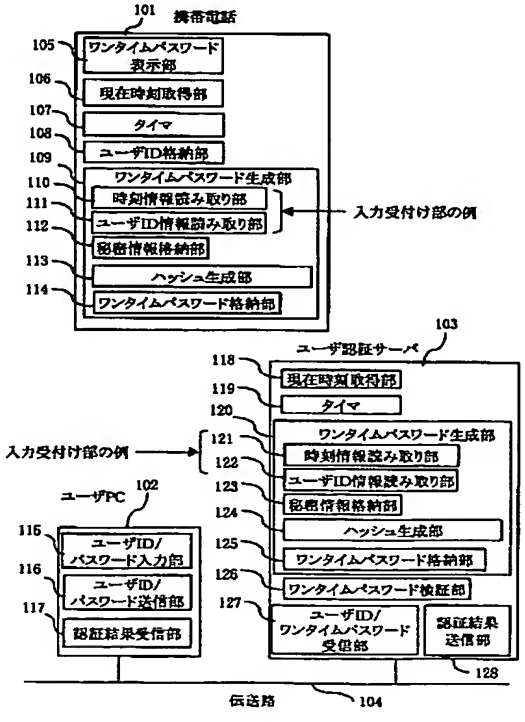
(22)出願日　平成13年２月28日(2001.2.28)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　米田　健
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

最終頁に続く

(54)【発明の名称】　ワンタイムパスワード認証システム及び携帯電話及びユーザ認証サーバ

(57)【要約】
【課題】　情報通信ネットワークシステムにおけるワンタイムパスワードを利用したユーザ認証に係り、ワンタイムパスワードの安全性を担保しつつ、秘密情報の管理を容易にすることを課題とする。
【解決手段】　携帯電話１０１のハッシュ生成部１１３で、ユーザＩＤと、現在時刻情報と、共通の秘密情報とを用いて、ハッシュ値を求め、ワンタイムパスワードを生成する。ユーザＰＣ１０２からユーザＩＤとワンタイムパスワードを受信したユーザ認証サーバ１０３は、ハッシュ生成部１２４で、受信したユーザＩＤと、現在時刻情報と、共通の秘密情報とを用いて、同様にワンタイムパスワードを生成し、ワンタイムパスワード検証部による検証に用いる。



【特許請求の範囲】

【請求項１】　ユーザ端末に接続するユーザ認証サーバと、携帯電話とからなるワンタイムパスワード認証システムであって、

携帯電話は、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有し、

ユーザ認証サーバは、（４）ユーザＩＤとワンタイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワンタイムパスワード受信部と、（５）携帯電話側秘密情報格納部で格納する秘密情報と同一の秘密情報を格納するサーバ側秘密情報格納部と、（６）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（７）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザＩＤ／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、

（８）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とするワンタイムパスワード認証システム。

【請求項２】　上記携帯電話側ハッシュ生成部は、携帯電話側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成し、そのＭＡＣをワンタイムパスワードとし、

上記サーバ側ハッシュ生成部は、サーバ側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとのＭＡＣを生成し、そのＭＡＣをワンタイムパスワードとすることを特徴とする請求項１記載のワンタイムパスワード認証システム。

【請求項３】　上記携帯電話は、ユーザＩＤと現在時刻情報との入力を受け付ける携帯電話側入力受付け部と、上記携帯電話側秘密情報格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、

上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、

上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報との入力を受け付けるサーバ側入力受付け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、

上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする請求項１記載のワンタイムパスワード認証システム。

【請求項４】　上記携帯電話は、現在時刻情報の入力を受け付ける携帯電話側入力受付け部と、上記携帯電話側秘密情報格納部と、ユーザＩＤを格納するユーザＩＤ格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、

上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、

上記ユーザＩＤ格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部から読み出しが可能で、かつ書き込みが不可能である構成を有し、

上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報との入力を受け付けるサーバ側入力受付け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、

上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする請求項１記載のワンタイムパスワード認証システム。

【請求項５】　上記携帯電話側ワンタイムパスワード生成部は、携帯電話に着脱可能なＩＣカードにより構成され、

ＩＣカードが携帯電話に装着されることにより、携帯電話側ハッシュ生成部が、ワンタイムパスワードを生成し、更に、ワンタイムパスワード表示部が、ワンタイムパスワードを表示することを特徴とする請求項４記載のワンタイムパスワード認証システム。

【請求項６】　携帯電話は、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証する携帯電話側現在時刻取得部を有し、

検証が成功した現在時刻情報により時刻調整する携帯電話側タイマとを有し、

携帯電話側ハッシュ生成部は、時刻調整された携帯電話側タイマが示す現在時刻情報を用い、

ユーザ認証サーバは、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証するサーバ側現在時刻取得部を有し、

検証が成功した現在時刻情報により時刻調整するサーバ側タイマとを有し、

携帯電話側ハッシュ生成部は、時刻調整されたサーバ側タイマが示す現在時刻情報を用いることを特徴とする請求項１記載のワンタイムパスワード認証システム。

【請求項７】　ワンタイムパスワード認証システムを構成する携帯電話であって、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有することを特徴とする携帯電話。

【請求項８】　ユーザ端末に接続し、ワンタイムパスワード認証システムを構成するユーザ認証サーバであって、（１）ユーザＩＤとワンタイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワンタイムパスワード受信部と、（２）秘密情報を格納するサーバ側秘密情報格納部と、（３）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（４）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザＩＤ／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、（５）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とするユーザ認証サーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、情報通信ネットワークシステムにおけるユーザ認証システムに関するものである。

【０００２】

【従来の技術】ワンタイムパスワード方式とは、利用者が頭で覚えているパスワードのかわりに、トークンと呼ばれる小さな携帯装置に表示されるパスワードを入力してユーザ認証を行う方式である（”Ｆｉｒｅｗａｌｌ ａｎｄ Ｉｎｔｅｒｎｅｔ Ｓｅｃｕｒｉｔｙ”，Ｗｉｌｌｉａｍ Ｒ．Ｃｈｅｓｗｉｃｋ，ｐｐ．１２０）。図１０は、トークンの外観を示す図である。図１１は、従来のワンタイムパスワード認証システムの概要を示す図である。

【０００３】図１２は、秘密情報の管理状態を示す図である。図に示すように、ユーザ毎にトークンを配布する必要がある。また、各トークンには、異なる秘密情報が格納され、その秘密情報は、ユーザ認証サーバのユーザＩＤ／秘密情報格納テーブルに登録される必要がある。

【０００４】図１３は、従来技術におけるワンタイムパスワード認証システムの構成を示す図である。図１４は、従来技術におけるワンタイムパスワード認証システムの処理フローを示す図である。続いて処理について説明する。まず、トークン１３０１では、タイマ１３０５から時刻情報を取得する（ステップＳ１７０１）。次にワンタイムパスワード生成部１３０７において、時刻情報と秘密情報格納部１３０６に格納されている秘密情報とからハッシュ関数等の一方向性関数を用いてワンタイムパスワードを生成する（ステップＳ１７０２）。生成されたワンタイムパスワードは、ワンタイムパスワード表示部１３０８に表示される（ステップＳ１７０３）。

【０００５】ＰＣのユーザは、ユーザＰＣ１３０２で起動しているアプリケーションのユーザＩＤ／パスワード入力部１３０９に、ユーザＩＤとワンタイムパスワードを入力する（ステップＳ１７０４）。入力されたユーザＩＤとワンタイムパスワードは、ユーザＩＤ／ワンタイムパスワード送信部１３１０より、ユーザ認証サーバ１３０３に伝送路１３０４経由で送信される（ステップＳ１７０５）。

【０００６】ユーザ認証サーバ１３０３は、ユーザＩＤとワンタイムパスワードを、ユーザＩＤ／ワンタイムパスワード受信部１３１２で受信すると（ステップＳ１７０６）、まず受け取ったユーザＩＤに対応する秘密情報をユーザＩＤ／秘密情報格納テーブル１３１６から選択し（ステップＳ１７０７）、タイマ１３１７から時刻情報を取得した後（ステップＳ１７０８）、ワンタイムパスワード生成部１３１３にて、時刻情報と秘密情報からワンタイムパスワードを生成する（ステップＳ１７０９）。ステップＳ１７０９にて生成されたワンタイムパスワードは、ワンタイムパスワード検証部１３１４において、受信したワンタイムパスワードと比較される（ステップＳ１７１０）。比較結果が一致すればユーザ認証成功であり、一致しなれば、失敗である。ユーザ認証サーバ１３０３は、ユーザ認証結果を認証結果送信部１３１５より、ユーザＰＣ１３０２に伝送路１３０４経由で送信する（ステップＳ１７１１）。

【０００７】ユーザＰＣ１３１２では、認証結果を認証結果受信部１３１１にて受信する（ステップＳ１７１２）。認証結果が成功であれば、業務処理を実行し（ステップＳ１７１４）、失敗であれば処理を終了する（ステップＳ１７１５）。

【０００８】クライアントサーバ方式を採用している情報通信システムにおいては、指紋やデジタル署名などの新しいユーザ認証方式を導入するためには、クライアントプログラムの大きな変更が必要である。一方トークンを用いたワンタイムパスワード方式では、クライアントプログラムで、ユーザ名とパスワードの入力を受け付ける際に、従来ユーザが頭で覚えているパスワードのかわりに、トークンに表示されるワンタイムパスワードが入力される。その違いをクライアントプログラムは区別する必要がない。したがって、クライアントプログラムの

変更が不要であるという長所がある。

【０００９】

【発明が解決しようとする課題】従来の方式においては、ワンタイムパスワード生成・表示装置（トークン）を携帯しなければならない。しかし、社内電話のＰＨＳ化、携帯電話の普及が進み、一人一台携帯電話を持つ環境において、更にトークンを携帯することは、煩わしい。

【００１０】また、従来の方式では、トークン毎に異なる秘密情報が必要であり、それらの秘密情報はすべてユーザ認証サーバに登録する必要があった。各秘密情報は、生成、登録の過程で機密に保護される必要がある。秘密情報の生成、登録作業はユーザの人数分実施する必要があり、その作業の間、秘密情報を機密に保つ手間は大きかった。上述の欠点を除くことを課題とする。

【００１１】

【課題を解決するための手段】本発明に係るワンタイムパスワード認証システムは、ユーザ端末に接続するユーザ認証サーバと、携帯電話とからなるワンタイムパスワード認証システムであって、携帯電話は、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有し、ユーザ認証サーバは、（４）ユーザＩＤとワンタイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワンタイムパスワード受信部と、（５）携帯電話側秘密情報格納部で格納する秘密情報と同一の秘密情報を格納するサーバ側秘密情報格納部と、（６）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（７）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザＩＤ／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、（８）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とする。

【００１２】上記携帯電話側ハッシュ生成部は、携帯電話側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとのＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を生成し、そのＭＡＣをワンタイムパスワードとし、上記サーバ側ハッシュ生成部は、サーバ側秘密情報格納部に格納する秘密情報を鍵として共通鍵暗号方式により、現在時刻情報と、ユーザＩＤとのＭＡＣを生成し、そのＭＡＣをワンタイムパスワードとすることを特徴とする。

【００１３】上記携帯電話は、ユーザＩＤと現在時刻情報との入力を受け付ける携帯電話側入力受付け部と、上記携帯電話側秘密情報格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報との入力を受け付けるサーバ側入力受付け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする。

【００１４】上記携帯電話は、現在時刻情報の入力を受け付ける携帯電話側入力受付け部と、上記携帯電話側秘密情報格納部と、ユーザＩＤを格納するユーザＩＤ格納部と、上記携帯電話側ハッシュ生成部とを含む携帯電話側ワンタイムパスワード生成部を有し、上記携帯電話側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有し、上記ユーザＩＤ格納部は、一度だけ書き込みが可能であり、書き込み後は携帯電話側ワンタイムパスワード生成部の外部から読み出しが可能で、かつ書き込みが不可能である構成を有し、上記ユーザ認証サーバは、ユーザＩＤと現在時刻情報との入力を受け付けるサーバ側入力受付け部と、上記サーバ側秘密情報格納部と、上記サーバ側ハッシュ生成部とを含むサーバ側ワンタイムパスワード生成部を有し、上記サーバ側秘密情報格納部は、一度だけ書き込みが可能であり、書き込み後はサーバ側ワンタイムパスワード生成部の外部からの読み出し及び書き込みが不可能である構成を有することを特徴とする。

【００１５】上記携帯電話側ワンタイムパスワード生成部は、携帯電話に着脱可能なＩＣカードにより構成され、ＩＣカードが携帯電話に装着されることにより、携帯電話側ハッシュ生成部が、ワンタイムパスワードを生成し、更に、ワンタイムパスワード表示部が、ワンタイムパスワードを表示することを特徴とする。

【００１６】携帯電話は、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証する携帯電話側現在時刻取得部を有し、検証が成功した現在時刻情報により時刻調整する携帯電話側タイマとを有し、携帯電話側ハッシュ生成部は、時刻調整された携帯電話側タイマが示す現在時刻情報を用い、ユーザ認証サ

ーバは、デジタル署名が付加された現在時刻情報を受信し、受信した現在時刻情報を検証するサーバ側現在時刻取得部を有し、検証が成功した現在時刻情報により時刻調整するサーバ側タイマとを有し、携帯電話側ハッシュ生成部は、時刻調整されたサーバ側タイマが示す現在時刻情報を用いることを特徴とする。

【００１７】本発明に係る携帯電話は、ワンタイムパスワード認証システムを構成する携帯電話であって、

（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有することを特徴とする。

【００１８】本発明に係るユーザ認証サーバは、ユーザ端末に接続し、ワンタイムパスワード認証システムを構成するユーザ認証サーバであって、（１）ユーザＩＤとワンタイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワンタイムパスワード受信部と、（２）秘密情報を格納するサーバ側秘密情報格納部と、（３）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（４）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザＩＤ／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、（５）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とする。

【００１９】

ハッシュ値　＝　Ｈａｓｈ（ユーザＩＤ‖時刻情報‖秘密情報）　式１

ユーザＩＤと時刻情報と秘密情報の間の記号は、結合を示している。Ｈａｓｈ（Ｘ）は、情報ＸのＨａｓｈ値を生成することを示す。つまり、上式はユーザＩＤ、時刻情報、秘密情報をすべて結合し、その結合した情報からＳＨＡ１ハッシュアルゴリズムに従い、ハッシュ値を計算する。生成された２０Ｂｙｔｅのバイナリハッシュ値を、Ｂａｓｅ６４により２８文字のキーボード入力可能文字列に変換し、その先頭８文字をワンタイムパスワード表示部１０５に表示する（ステップＳ３０２）。なお、ハッシュ値の生成方法としてＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を用いることも可能である。その場合、秘密情報をＭＩＳＴＹやＤＥＳなどの共通鍵暗号方式の鍵とする。そして、ユーザＩＤと時刻情報の結合情報から、上記鍵を利用して、ＭＡＣを生成する。このＭＡＣをハッシュ値として利用する。

【発明の実施の形態】実施の形態１．本実施の形態では、携帯電話、認証サーバに共通かつ唯一の秘密情報を格納する。つまり、ユーザ認証システムに用いられるすべての携帯電話と、認証サーバが単一の秘密情報を共有する。そして、携帯電話、認証サーバの時刻を同期させ、ユーザＩＤと時刻情報と秘密情報からワンタイムパスワードを生成する。ワンタイムパスワード生成部は、秘密情報格納部と、入力受付部と、ハッシュ生成部と、ハッシュ格納部を有している。秘密情報格納部は、一度だけ書き込みが可能で、以降外部からの読み出し、書き込みが不可であり、入力受付部は、外部から２つの入力のみを受け付け、ハッシュ生成部は、２つの入力と秘密情報格納部に格納された秘密情報とからハッシュ値を生成する。ハッシュ格納部は、そのハッシュを読み出し可能なように格納する。

【００２０】図１は、実施の形態１におけるユーザ認証システムの構成を示す図である。図２は、実施の形態１におけるユーザ認証システムの概要を示す図である。図３は、実施の形態１におけるユーザ認証システムの処理フローを示す図である。まず、携帯電話１０１では、ワンタイムパスワードを生成する（ステップＳ３０１）。

【００２１】図４は、ワンタイムパスワード生成の詳細フローを示す図である。まず、タイマ１０７から時刻情報を取得する（ステップＳ４０１）。時刻情報は現在時刻を分単位で表現したものである。次に、ユーザＩＤ格納部１０８に格納されているユーザＩＤを取得する（ステップＳ４０２）。ハッシュ生成部１１３において、ステップＳ４０１で取得した時刻情報と、ステップＳ４０２で取得したユーザＩＤと、秘密情報格納部１１２に格納されている秘密情報とからハッシュ関数等の一方向性関数を用いてワンタイムパスワードを生成する（ステップＳ４０３）。具体的な生成式を以下に示す。

【００２２】ＰＣのユーザは、ユーザＰＣ１０２で起動しているアプリケーションのユーザＩＤ／パスワード入力部１１５に、ユーザＩＤとワンタイムパスワードを入力する（ステップＳ３０３）。入力されたユーザＩＤとワンタイムパスワードは、ユーザＩＤ／ワンタイムパスワード送信部１１６より、ユーザ認証サーバ１０３に伝送路１０４経由で送信される（ステップＳ３０４）。

【００２３】ユーザ認証サーバ１０３は、ユーザＩＤとワンタイムパスワードを、ユーザＩＤ／タイムパスワード受信部１２７で受信すると（ステップＳ３０５）、ワンタイムパスワードを生成する（ステップＳ３０６）。図４に示すように、タイマ１１９から時刻情報を取得した後（ステップＳ４０１）、受信したユーザＩＤをユーザＩＤ情報読み取り部で読み取り、秘密情報格納部１２３から秘密情報を取得する。そして、ハッシュ生成部１２４で、時刻情報と、ユーザＩＤと、秘密情報時刻情報

と秘密情報とから上式によりハッシュ値を計算し、生成された２０Ｂｙｔｅのバイナリハッシュ値を、Ｂａｓｅ６４により２８文字のキーボード入力可能文字列に変換し、その先頭８文字をワンタイムパスワードとする（ステップＳ４０３）。ステップＳ４０３にて生成されたワンタイムパスワードは、ワンタイムパスワード格納部１２５に格納される。

【００２４】ワンタイムパスワード検証部１２６は、ワンタイムパスワード格納部１２５からワンタイムパスワードを取得すると、受信したワンタイムパスワードと比較する（ステップＳ３０７）。比較結果が一致すればユーザ認証成功であり、一致しなれば、時刻情報を一分前のものとし、ワンタイムパスワードを計算し直す。その結果と一致すればユーザ認証成功であり、それでも一致しない場合は失敗とする。ユーザ認証サーバ１０３は、ユーザ認証結果を認証結果送信部１２８より、ユーザＰＣ１０２に伝送路１０４経由で送信する（ステップＳ３０９）。

【００２５】ユーザＰＣ１０２では、認証結果を認証結果受信部１１７にて受信する（ステップＳ３１０）。認証結果が成功であれば、業務処理を実行し（ステップＳ３１２）、失敗であれば処理を終了する（ステップＳ３１３）。

【００２６】上述のように、ワンタイムパスワード生成部１０９，１２０は同一構成を有する。一度だけ書き込みが可能で、書込み後は、外部からの読み出し、書き込みが不可である秘密情報格納部１２１と、外部から時刻情報の入力を受け付ける時刻情報読み取り部１１０，１２１と外部からユーザＩＤ情報の入力を受け付けるユーザＩＤ情報読み取り部と、時刻情報、ユーザＩＤ、秘密情報からハッシュを生成するハッシュ生成部１１３，１２４と外部から唯一読み出し可能な情報を格納するワンタイムパスワード格納部とを含んでいる。

【００２７】また、タイマ１１７，１１９は同期させる。現在時刻情報は、ＮＨＫの時報情報や、電波によるデジタル時刻情報配信サービスがあるため、それらの時刻情報を１日一回現在時刻取得部で受信し、タイマの時刻のずれを修正する。ユーザ認証サーバは、情報通信ネットワークに接続されているので、情報通信ネットワーク経由のＮＴＰ（Ｎｅｔｗｏｒｋ　Ｔｉｍｅ　Ｐｒｏｔｏｃｏｌ）等の時刻同期機能によりタイマのずれを修正してもよい。

【００２８】本実施の形態による効果について説明する。まず、携帯電話に表示されるワンタイムパスワードは、ユーザＩＤ、時刻情報、秘密情報のハッシュ値であるので、ユーザＩＤと時刻情報のいずれかが異なればワンタイムパスワードは異なる値となる。また、ユーザ認証サーバでは、ユーザＩＤ，時刻情報、秘密情報から同一のハッシュ値を再現できる。また、秘密情報は、ユーザの携帯電話、ユーザ認証サーバで共通のものを使っているが、外部からの読み出しが困難なワンタイムパスワード生成部により機密に保たれている。したがって、第三者が他人のワンタイムパスワードを推定することは困難である。したがって、本実施の形態で利用するワンタイムパスワードは安全性が確保されている。

【００２９】また、本実施の形態では、携帯される携帯電話にワンタイムパスワードが表示されるため、新たにワンタイムパスワード生成表示用のトークンを携帯する必要がない。そして、機密に保持する必要があるデータは、共通に利用される秘密情報のみであり、ユーザ認証サーバに、一度この秘密情報を登録すれば、ユーザ数が増加しても新たに登録する秘密情報はない。

【００３０】実施の形態２．図５は、実施の形態２におけるワンタイムパスワード生成部の構成を示す図である。本実施の形態では、携帯電話で利用するワンタイムパスワード生成部として、一度だけ書き込みが可能で、書込み後外部からの読み出し、書き込みが不可の秘密情報格納部５０６と、一度だけ書き込みが可能で、書込み後外部から読み出しは可能であるが、書き込みは不可であるユーザＩＤ格納部５０３と、唯一の外部からの入力情報として時刻情報を受け付ける時刻情報読み取り部５０２、および実施の形態１におけるハッシュ生成部１１３，１２４と同一のハッシュ生成部５０４、ワンタイムパスワード格納部５０５から構成されるワンタイムパスワード生成部５０１を利用する。実施の形態１と異なるのは、ワンタイムパスワード生成部において、ユーザＩＤ情報を外部から読み取るのではなく、ワンタイムパスワード生成部の内部に、読み取り可、変更不可の状態で格納されたユーザＩＤ情報を利用する点である。

【００３１】本実施の形態の効果について説明する。悪意のある者が、携帯電話を不正に分解し、ワンタイムパスワード生成部を入手しても、外部からワンタイムパスワード生成部に入力できる情報は、時刻情報に限られている。したがって、任意のユーザＩＤに対応する将来の時刻のワンタイムパスワードを不正に入手することは困難となり、携帯電話の不正分解に対して、より安全なワンタイムパスワード認証システムを構築することができる。

【００３２】実施の形態３．ここでは、図５のワンタイムパスワード生成部をＩＣカードに持たせ、携帯電話にＩＣカードを差し込むと携帯電話のディスプレイにワンタイムパスワードが表示される形態について説明する。図６は、実施の形態３における携帯電話とＩＣカードの構成を示す図である。ワンタイムパスワード表示部６０２、現在時刻取得部６０３、タイマ６０４は図１における前述の１０５，１０６，１０７の要素と同一の機能を有する。ＩＣカード挿入部６０５は、物理的なＩＣカード差込口と、ＩＣカードとの情報交換のインターフェースを提供する。ＩＣカード６０６は、時刻情報読み取り部６０７，ユーザＩＤ格納部６０８，ワンタイムパスワ

ード生成部６０９，ワンタイムパスワード６１０，秘密情報格納部６１１から構成され、それぞれ、前述の５０２，５０３，５０４，５０５，５０６の要素と同一の機能を有する。

【００３３】ワンタイムパスワード生成の処理において、タイマ６０４の時刻情報は、時刻情報読み取り部６０７により読み取られ、それぞれユーザＩＤ格納部６０８と秘密情報格納部６１１に格納されているユーザＩＤ情報と秘密情報とともに、ハッシュ生成部６０９におけるハッシュ生成に用いられる。生成されたハッシュ値は、ワンタイムパスワード格納部６１０にワンタイムパスワードとして格納され、ＩＣカード挿入部６０５を通してワンタイムパスワード表示部６０２に表示される。

【００３４】本実施の形態の効果について説明する。例えば、Ａ社の提供するオンラインショッピングシステムと、Ｂ社の提供するオンラインバンキングシステムでユーザ認証が必要となる場合には、Ａ社とＢ社は、それぞれ互いの秘密情報管理にユーザ認証の安全性を依存させることをさけるために、それぞれに異なる秘密情報を保持する。その結果、異なるユーザ認証サーバを用いることが必要となる。このような場合に、ユーザ認証サーバと共有する秘密情報を携帯電話毎に内蔵することとすると、それぞれのシステムにアクセスする際に、アクセスするシステムに対応する秘密情報を持つ携帯電話を選択して利用しなくてはならない。その結果、複数の形態電話を保有することとなり、コストが高く、利便性も悪くなる。しかし、本実施の形態のように、ＩＣカードに秘密情報を格納するようにすれば、Ａ社、Ｂ社のシステムを両方利用するユーザは、Ａ社用のＩＣカードとＢ社用のＩＣカードを２つもち、それぞれのシステムにアクセスする際に、対応するＩＣカードを携帯電話に挿入して表示されるワンタイムパスワードを利用することができる。その結果、単一の携帯電話で、ユーザ認証を実行するユーザ認証サーバ毎に、異なる秘密情報を割り当てることが可能となり、コストは低く、利便性も向上する。

【００３５】実施の形態４．本実施の形態では、同期の元となる時刻情報を発信する時刻情報発信サーバにおいて、時刻の情報にデジタル署名を付与し、時刻携帯電話とユーザ認証サーバは現在時刻取得の際にその署名を検証する。図７は、実施の形態４における時刻情報発信サーバの構成図である。図８は、実施の形態４における現在時刻取得部の構成図である。図９は、実施の形態４における現在時刻取得処理のフローを示す図である。

【００３６】時刻情報発信サーバ７０１では、タイマ７０２から現在時刻情報を取得すると（ステップＳ９０１）、秘密鍵情報格納部７０５に格納された公開鍵暗号方式の秘密鍵を用いて、署名生成部７０３により、時刻情報のデジタル署名を生成し、そのデジタル署名を時刻情報に付加する（ステップＳ９０２）。デジタル署名付き現在時刻情報は、現在時刻情報発信部７０４より、電波により発信される（ステップＳ９０３）。

【００３７】発信されたデジタル署名付き現在時刻情報は、携帯電話とユーザ認証サーバそれぞれの現在時刻情報受信部８０２で受信される。（ステップＳ９０４）その後、公開鍵格納部８０４に格納された公開鍵情報、つまり時刻情報発信サーバの秘密鍵情報に対応する公開鍵情報を用いて、署名検証部８０３により、デジタル署名の検証が行われる（Ｓ９０５）。検証に失敗した場合は、不正な時刻情報発信サーバにより発信された時刻情報であるか、途中で改ざんされた時刻情報であると判断し、受信した時刻情報を破棄する。検証に成功すれば、正しい時刻情報サーバから改ざんされずに送られてきた時刻情報と判断し、時刻情報を受け取る。受け取った時刻情報が、現在の携帯電話、認証サーバのタイマの示す時刻情報と、指定された範囲のずれを生じさせている場合には、携帯電話、認証サーバのタイマの時刻情報を、受信した時刻情報の値に修正する。但し、指定された時間以上ずれている場合には、携帯電話、認証サーバのタイマに異常があると判断し、エラーとする。

【００３８】時刻情報発信サーバのデジタル署名付き時刻情報の発信間隔及び、受信側でのタイマ時刻修正を発生させる時間のずれの範囲については、任意の値に設定できる。例えば、時刻情報発信サーバのデジタル署名付き時刻情報の発信は、一日一回とし、受信側では、時刻情報とのずれが３０秒以上５分以内のときは、受信した時刻情報に自らのタイマ情報を修正するように設定できる。

【００３９】公開鍵暗号方式のアルゴリズムとしては、ＲＳＡ、楕円暗号等アルゴリズムが使用可能である。

【００４０】本実施の形態の効果について説明する。携帯電話、ユーザ認証サーバのタイマを、標準時刻に同期する際に、信頼できる発信元からの改ざんされていない時刻情報を用いることができるので、安全な時刻同期が可能となる。

【００４１】

【発明の効果】本発明においては、同期する時刻と、共通の秘密情報に基づいて、ユーザＩＤに対応するワンタイムパスワードを生成し、秘密情報の読み取りが不可である構成としているので、ワンタイムパスワードの安全性を担保しつつ、秘密情報の管理を容易にすることができる。また、携帯電話でワンタイムパスワードを生成するので、トークンを携帯する必要がなくなる。

【００４２】ワンタイムパスワード生成部は、ユーザＩＤを内部に保持し、入力するパラメータを時刻情報に限っているので、携帯電話の分解によるワンタイムパスワードの不正な生成を阻止することができる。

【００４３】ワンタイムパスワード生成部を、携帯電話に着脱可能なＩＣカードにおいて実現するので、ユーザ認証サーバに対応するＩＣカードを用いることにより、複数のユーザ認証サーバのサービスを簡単に享受するこ

とができる。

【００４４】デジタル認証された現在時刻により時刻を修正するので、常に適正な時刻情報に基づくワンタイムパスワードが生成されるようになる。

【図面の簡単な説明】

【図１】　実施の形態１におけるユーザ認証システムの構成を示す図。

【図２】　実施の形態１におけるユーザ認証システムの概要を示す図。

【図３】　実施の形態１におけるユーザ認証システムの処理フローを示す図。

【図４】　ワンタイムパスワード生成の詳細フローを示す図。

【図５】　実施の形態２におけるワンタイムパスワード生成部の構成を示す図。

【図６】　実施の形態３における携帯電話とＩＣカードの構成を示す図。

【図７】　実施の形態４における時刻情報発信サーバの構成図。

【図８】　実施の形態４における現在時刻取得部の構成図。

【図９】　実施の形態４における現在時刻取得処理のフローを示す図。

【図１０】　トークンの外観を示す図。

【図１１】　従来のワンタイムパスワード認証システムの概要を示す図。

【図１２】　秘密情報の管理状態を示す図。

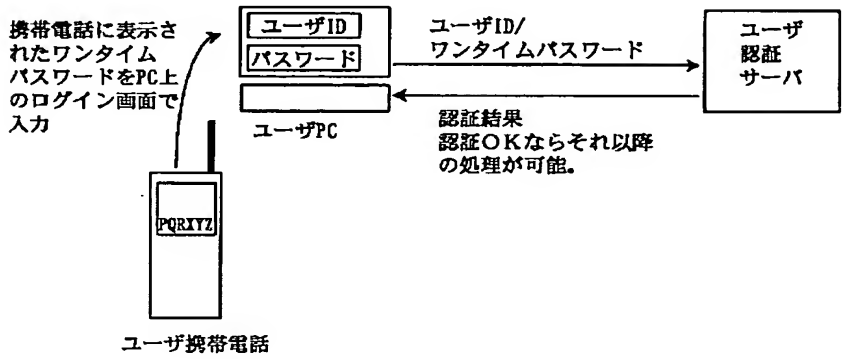
【図１３】　従来技術におけるワンタイムパスワード認証システムの構成を示す図。

【図１４】　従来技術におけるワンタイムパスワード認証システムの処理フローを示す図。

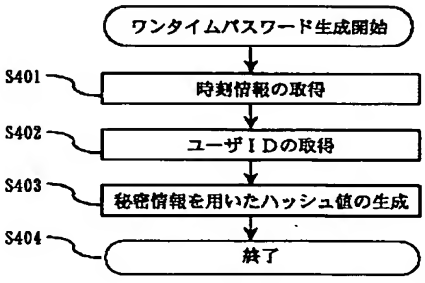
【符号の説明】

１０１　携帯電話、１０２　ユーザＰＣ、１０３　ユーザ認証サーバ、１０４伝送路、１０５　ワンタイムパスワード表示部、１０６　現在時刻取得部、１０７　タイマ、１０８　ユーザＩＤ格納部、１０９　ワンタイムパスワード生成部、１１０　時刻情報読み取り部、１１１　ユーザＩＤ情報読み取り部、１１２秘密情報格納部、１１３　ハッシュ生成部、１１４　ワンタイムパスワード格納部、１１５　ユーザＩＤ／パスワード入力部、１１６　ユーザＩＤ／パスワード送信部、１１７　認証結果受信部、１１８　現在時刻取得部、１１９　タイマ、１２０　ワンタイムパスワード生成部、１２１　時刻情報読み取り部、１２１ユーザＩＤ情報読み取り部、１２３　秘密情報格納部、１２４　ハッシュ生成部、１２５　ワンタイムパスワード格納部、１２６　ワンタイムパスワード検証部、１２７　ユーザＩＤ／ワンタイムパスワード受信部、１２８　認証結果送信部、５０１　ワンタイムパスワード生成部、５０２　時刻情報読み取り部、５０３ユーザＩＤ格納部、５０４　ハッシュ生成部、５０５　ワンタイムパスワード格納部、５０６　秘密情報格納部、６０１携帯電話、６０２　ワンタイムパスワード表示部、６０３　現在時刻取得部、６０４　タイマ、６０５　ＩＣカード挿入部、６０６　ＩＣカード、６０７　時刻情報読み取り部、６０８　ユーザＩＤ格納部、６０９　ハッシュ生成部、６１０　ワンタイムパスワード格納部、６１１　秘密情報格納部、７０１　時刻情報発信サーバ、７０２　タイマ、７０３署名生成部、７０４　現在時刻発信部、７０５　秘密鍵格納部、８０１　現在時刻取得部、８０２　現在時刻情報受信部、８０３　署名検証部、８０４　公開鍵格納部、８０５　現在時刻格納部。

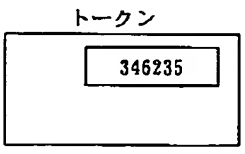
【図２】



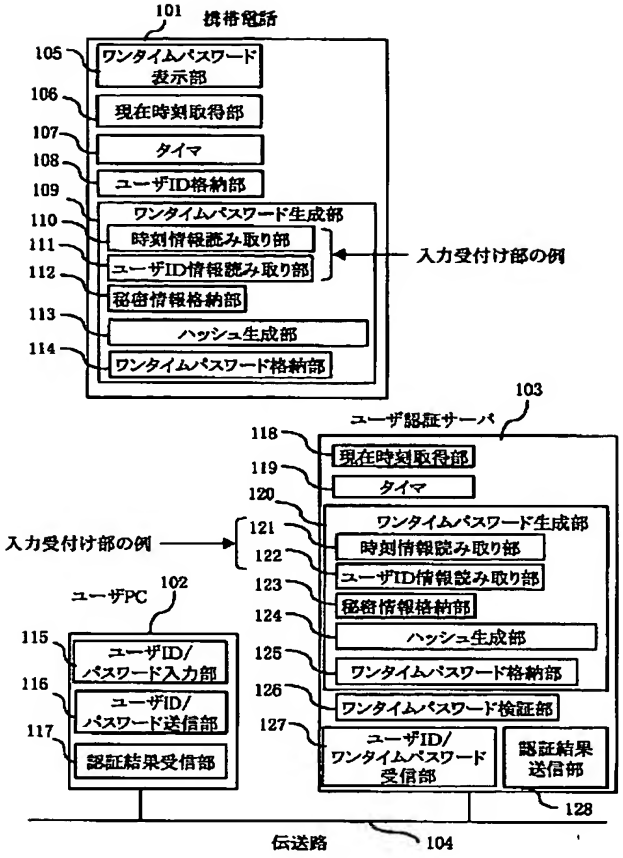
【図４】



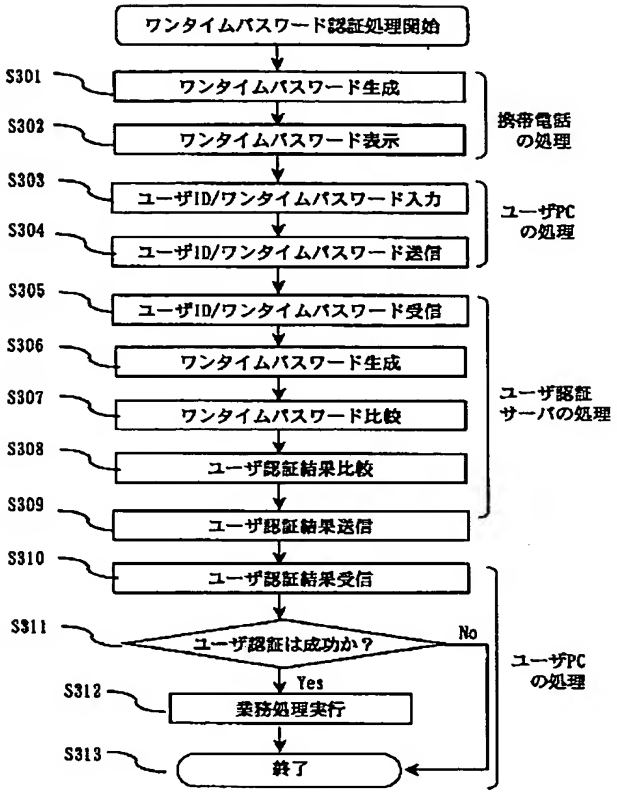
【図１０】



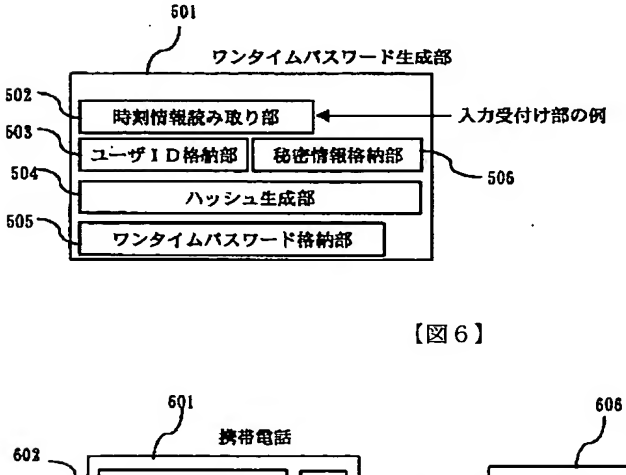
【図１】


101 携帯電話
105 ワンタイムパスワード表示部
106 現在時刻取得部
107 タイマ
108 ユーザID格納部
109 ワンタイムパスワード生成部
110 時刻情報読み取り部
111 ユーザID情報読み取り部
112 秘密情報格納部
113 ハッシュ生成部
114 ワンタイムパスワード格納部
入力受付け部の例
103 ユーザ認証サーバ
118 現在時刻取得部
119 タイマ
120 ワンタイムパスワード生成部
121 時刻情報読み取り部
122 ユーザID情報読み取り部
123 秘密情報格納部
124 ハッシュ生成部
125 ワンタイムパスワード格納部
126 ワンタイムパスワード検証部
127 ユーザID/ワンタイムパスワード受信部
認証結果送信部
128
入力受付け部の例
ユーザPC 102
115 ユーザID/パスワード入力部
116 ユーザID/パスワード送信部
117 認証結果受信部
伝送路 104

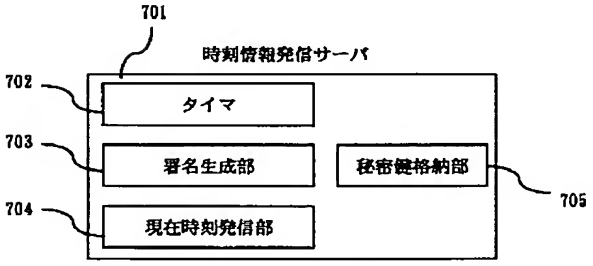
【図３】


ワンタイムパスワード認証処理開始
S301 ワンタイムパスワード生成
S302 ワンタイムパスワード表示
携帯電話の処理
S303 ユーザID/ワンタイムパスワード入力
S304 ユーザID/ワンタイムパスワード送信
ユーザPCの処理
S305 ユーザID/ワンタイムパスワード受信
S306 ワンタイムパスワード生成
S307 ワンタイムパスワード比較
S308 ユーザ認証結果比較
S309 ユーザ認証結果送信
ユーザ認証サーバの処理
S310 ユーザ認証結果受信
S311 ユーザ認証は成功か？
No
Yes
S312 業務処理実行
S313 終了
ユーザPCの処理

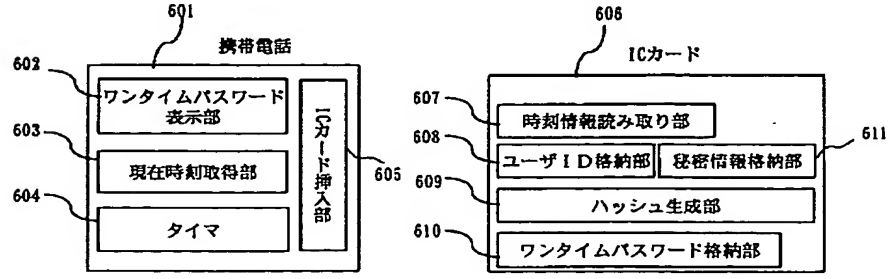
【図５】


501
ワンタイムパスワード生成部
502 時刻情報読み取り部
入力受付け部の例
503 ユーザＩＤ格納部
秘密情報格納部
506
504 ハッシュ生成部
505 ワンタイムパスワード格納部

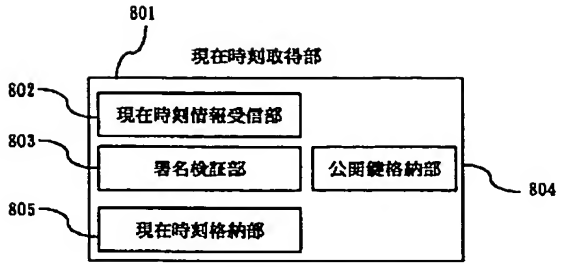
【図７】


701
時刻情報発信サーバ
702 タイマ
703 署名生成部
秘密鍵格納部
705
704 現在時刻発信部

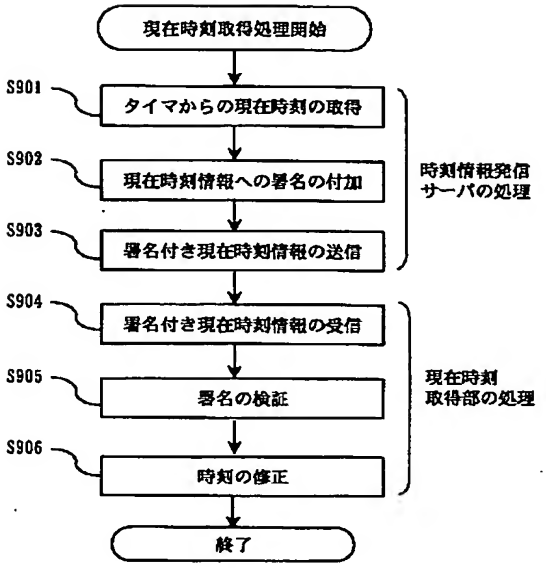
【図６】


601
携帯電話
602 ワンタイムパスワード表示部
603 現在時刻取得部
604 タイマ
ICカード挿入部
605
606
ICカード
607 時刻情報読み取り部
608 ユーザＩＤ格納部
秘密情報格納部
611
609 ハッシュ生成部
610 ワンタイムパスワード格納部

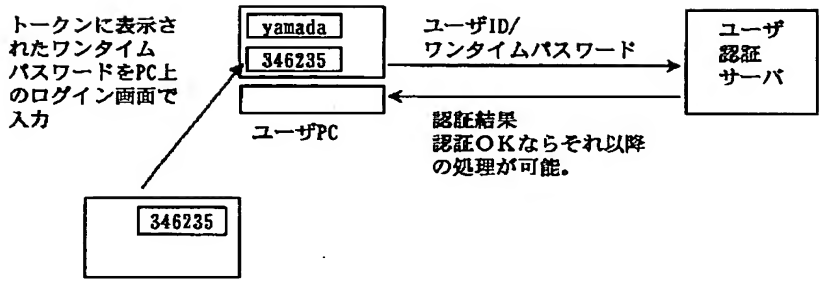
【図８】


801
現在時刻取得部
802
現在時刻情報受信部
803
署名検証部
公開鍵格納部
804
805
現在時刻格納部

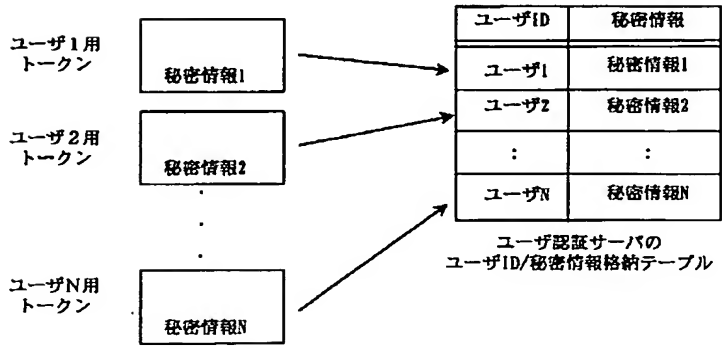
【図９】


現在時刻取得処理開始
S901
タイマからの現在時刻の取得
S902
現在時刻情報への署名の付加
S903
署名付き現在時刻情報の送信
時刻情報発信サーバの処理
S904
署名付き現在時刻情報の受信
S905
署名の検証
S906
時刻の修正
現在時刻取得部の処理
終了

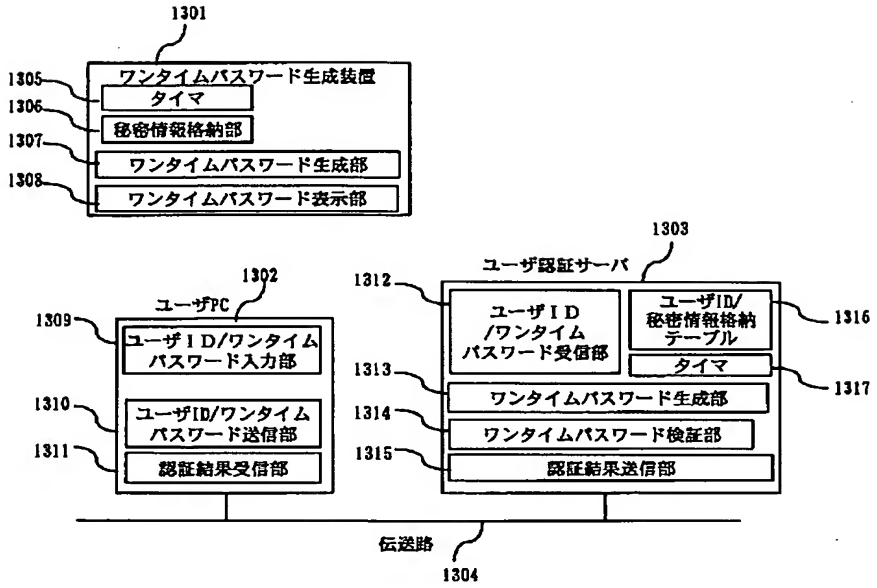
【図１１】


トークンに表示されたワンタイムパスワードをPC上のログイン画面で入力
yamada
346235
ユーザPC
ユーザID/
ワンタイムパスワード
ユーザ認証サーバ
認証結果
認証ＯＫならそれ以降の処理が可能。
346235
トークン

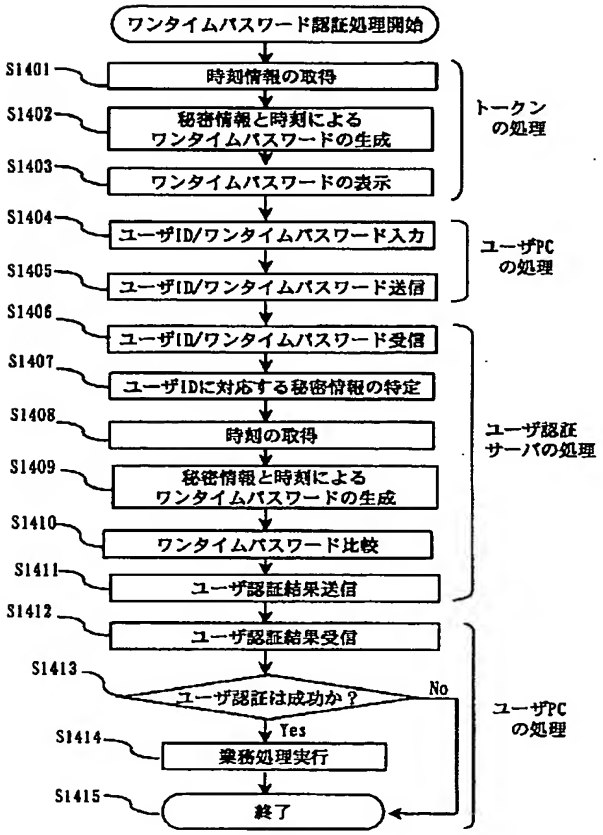
【図１２】


ユーザ１用トークン
秘密情報1
ユーザ２用トークン
秘密情報2
ユーザN用トークン
秘密情報N
ユーザID
秘密情報
ユーザ1
秘密情報1
ユーザ2
秘密情報2
:
:
ユーザN
秘密情報N
ユーザ認証サーバの
ユーザID/秘密情報格納テーブル

【図１３】


1301
ワンタイムパスワード生成装置
1305
タイマ
1306
秘密情報格納部
1307
ワンタイムパスワード生成部
1308
ワンタイムパスワード表示部
1303
ユーザ認証サーバ
1302
ユーザPC
1309
ユーザＩＤ/ワンタイム
パスワード入力部
1310
ユーザID/ワンタイム
パスワード送信部
1311
認証結果受信部
1312
ユーザＩＤ
/ワンタイム
パスワード受信部
ユーザID/
秘密情報格納
テーブル
1316
タイマ
1317
1313
ワンタイムパスワード生成部
1314
ワンタイムパスワード検証部
1315
認証結果送信部
伝送路
1304

【図１４】


ワンタイムパスワード認証処理開始
S1401
時刻情報の取得
S1402
秘密情報と時刻による
ワンタイムパスワードの生成
S1403
ワンタイムパスワードの表示
トークン
の処理
S1404
ユーザID/ワンタイムパスワード入力
S1405
ユーザID/ワンタイムパスワード送信
ユーザPC
の処理
S1406
ユーザID/ワンタイムパスワード受信
S1407
ユーザIDに対応する秘密情報の特定
S1408
時刻の取得
S1409
秘密情報と時刻による
ワンタイムパスワードの生成
S1410
ワンタイムパスワード比較
S1411
ユーザ認証結果送信
ユーザ認証
サーバの処理
S1412
ユーザ認証結果受信
S1413
ユーザ認証は成功か？
No
Yes
S1414
業務処理実行
S1415
終了
ユーザPC
の処理

フロントページの続き

(51) Int.Cl.[7]	識別記号	FI	テーマコード（参考）
		H04Q 7/04	B

Fターム（参考） 5B085 AE01 AE23 BG07
5J104 AA07 AA09 AA16 EA03 KA01
KA03 KA21 LA01 LA06 MA01
NA02 NA05 NA12 NA35 NA36
PA10
5K067 AA21 BB04 BB21 BB34 DD17
EE02 EE16 FF02 HH22 HH36
KK15